(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 881 560 A2

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
02.12.1998 Bulletin 1998/49

(51) Int. Cl.^{6}: **G06F 1/00**, G06F 3/06

(21) Application number: 98109862.7

(22) Date of filing: 29.05.1998

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 29.05.1997 JP 140029/97

(71) Applicant: Hitachi, Ltd.
Chiyoda-ku, Tokyo 101-8010 (JP)

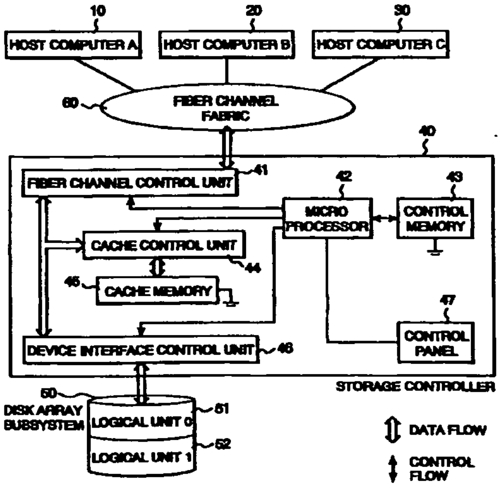
(72) Inventors:
- Sanada, Akemi
Minamiashigara-shi Kanagawa-ken 250-0113 (JP)
- Nakano, Toshio
Chigasaki-shi, Kanagawa-ken 253-0022 (JP)
- Iwasaki, Hidehiko
Hiratsuka-shi, Kanagawa-ken 254-0905 (JP)
- Sato, Masahiko
Odawara-shi, Kanagawa-ken 250-0217 (JP)
- Muraoka, Kenji
Odawara-shi, Kanagawa-ken 250-0866 (JP)
- Takamoto, Kenichi
Odawara-shi, Kanagawa-ken 250-0874 (JP)
- Kobayashi, Masaaki
Odawara-shi, Kanagawa-ken 256-0816 (JP)

(74) Representative:
Strehl Schübel-Hopf & Partner
Maximilianstrasse 54
80538 München (DE)

(54) Fibre channel connection storage controller

(57) N_Port_Name information capable of distinctly identifying a host computer has seen set in a microprocessor 42 of a storage controller 40 prior to start-up of host computers 10, 20, 30; upon startup of the host computers 10, 20, 30, when the storage controller 40 receives a frame issued, then the microprocessor 42 operates to perform comparison for determining whether the N_Port_Name information stored in the frame has been already set in the microprocessor 42 and registered to the N_Port_Name list within a control table maintained. When such comparison results in match, then continue execution of processing based on the frame instruction; if comparison results in failure of match, then reject any request.

FIG. 1



Printed by Xerox (UK) Business Services
2.16.6/3.4

Description

BACKGROUND OF THE INVENTION

The present invention relates to storage control apparatus with ANSIX3T11-standardized fiber channels as an interface with its upper-level or "host" computers, and more particularly to a storage controller device which is employable in a computer system including a host computer and a storage control device plus a storage unit operable under control of the storage controller and which is for elimination of unauthorized access attempts upon issuance of a request to access the storage unit as sent from the host computer to the storage controller.

Conventionally, with regard to elimination or determent of unauthorized or illicit access attempts over networks, a variety of approaches are known and proposed until today.

One typical prior known approach to deterring unauthorized access has been disclosed in Published Unexamined Japanese Patent Application ("PUJPA") No. 3-152652, wherein a network security system between computer systems supporting the TCP/IP protocol includes a memory device for storage of predefined identification (ID) information of those users who are authorized to log-in the network. The security system has a function of interrupting or disenabling any connection to the network whenever an unauthorized person attempts to log-in the network for invasion or "hacking" purposes.

Another approach has been disclosed in PUJPA No. 63-253450, wherein the central processing device disclosed comes with an operating system that is designed to monitor or "pilot" entry of user ID, password and online address data thereby deterring any unauthorized access to resource files on disk drive units.

Still another approach is based on the "ESCON" interface architecture available from IBM corp., which is designed so that by utilizing the fact that a host computer stores therein a logical address thereof as the source address of the host computer in the form of a frame and transmits the same to a storage controller device, the storage controller has a function of checking whether an incoming logical address in such frame matches a logical address that has been preset in the storage controller.

Any one of the prescribed prior art approaches are not more than a mere unauthorized access elimination means that is inherently directed to those interfaces with a single type of layer mounted on a host logical layer.

However, the ANSIX3T11-standardized fiber channel is the "network type" architecture, which is capable of providing the host logical layer with various built-in layers mountable thereon, such as for example TCP/IP, SCSI, ESCON, IPI and the like. More specifically, since the buffer contents are to be moved from one device to another in a way independent of the data format and contents, it may offer logical compatibility with other interface configurations and therefore remains physically accessible without suffering from any particular limitations. Especially, in a storage system including this fiber channel and a storage device with a plurality of storage regions such as a disk array device or "subsystem," the storage regions are usable in common by an increased number of host computers. Accordingly, the prior art unauthorized access determent schemes remain insufficient in performance and reliability. A need thus exists for achievement of secrecy protection based on users' intentional security setup.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a fiber channel connection storage control device adapted for use in a computer system which employs an ANSIX3T11-standardized fiber channel as an interface between one or more host computers and a storage control device and which includes host computers and a storage control device plus more than one storage device operable under control of the storage control device, wherein the fiber channel connection storage control device has a security function of, in the environment capable of physically receiving any access from the host computers, eliminating or deterring unauthorized access attempts from the host computers to the storage control device, which did not have any means for rejecting unauthorized access from host computers.

Another object of the present invention is to provide a fiber channel connection storage control device having a scheme capable of readily managing an accessible host computer or computers for elimination or determent of any unauthorized access from such host computers.

According to the present invention, the foregoing objects may be attainable in a way such that N_Port_Name information of an accessible host computer or computers which information distinctly identifies each host computer in a one-by-one basis is set in the storage control device for comparison with N_Port_Name information as stored in a frame to be sent from a host computer to thereby determine whether a presently desired access attempt is permissible or not.

One practical feature of the present invention in order to attain the prescribed objects is to have a means for inputting by use of a panel or the like the N_Port_Name information that is the information being issued from a host computer for distinct identification of the host computer, and then for storing such input information in a control memory of the storage control device as a control table. In this case, it will be desirable that the storage control device has a means for permanently storing therein the information until it is reset or updated.

And, by arranging the control table to be stored in a non-volatile control memory, it becomes possible to protect the management information even upon occurrence of any possible power supply failure or interruption.

In accordance with another practical feature of the present invention, after start-up of the host computer, the host computer generates and issues a frame that stores therein N_Port_Name information to the storage control device; the storage control device has means for comparing, when the storage control device receives this information, the maintained N_Port_Name information for distinct identification of the host computer to the N_Port_Name information as stored in the received frame: If the comparison results in a match between the two, then continue to execute the processing based on an instruction of the frame received; alternatively, if the comparison tells failure in match then return to the host computer an LS_RJT frame which rejects the presently received frame. It is thus possible for the storage control device to inhibit or deter any unauthorized access from the host computer.

A further practical feature of the present invention lies in presence of a means for setting N_Port_Name information items which are greater in number than or equal to a physical number of host interface units (ports) as owned by the storage control device. More specifically, a means is specifically provided for setting a plurality of N_Port_Name information items per port. This makes it possible to accommodate a multi-logical path configuration upon either a fiber channel fabric or a multi-logical path configuration upon switch connections.

Further, in a system having many magnetic disk volume parts such as a disk array device and also having a plurality of channel path routes, the system has manager means for performing management--within the storage control device in a one-to-one correspondence relation per channel path route--of storage regions under control of the storage control device, including a logical unit number (LUN)-based logical disk extent, a physical volume extent, a RAID group-based logical disk extent and the like, versus ports of the storage control device and N_Port_Name information of a host computer(s). This may enable users to deter an unauthorized access attempt per storage region, which in turn leads to achievement of more precise access management.

Furthermore in the present invention, even where the storage device under control of the storage control device is any one of an optical disk drive, magneto-optical (MO) disk drive and magnetic tape device as well as a variety of types of library devices of them, the storage control device has means for performing table based management and the storage information of a control table-based manager/holder means for dealing with the correspondence among the N_Port_Name information of an accessible host computer, ports of the storage control device, and the storage device, and further handling the correspondence management of media in the case of library apparatus, while simultaneously having a means for comparing, upon receipt of a frame as sent thereto, the information within the frame to the information in the control table, thereby eliminating unauthorized access attempts from host computers.

Moreover, the present invention comprises means for protecting the management information through inputting of a password upon setup of the information under management of the storage control device using a panel or the like. With such an arrangement, it is possible for users to eliminate any fraudulent registration of the information and also unauthorized resetting of the same. In addition, the users are capable of readily deter any unauthorized access by merely setting such management information thus reducing workloads on the users.

It should be noted that in the present invention, the means for setting the information as managed by the storage control device may be designed so that the use of the panel or the like is replaced with use of a utility program or programs of host computers to attain the intended setup operation.

In accordance with the present invention, in a computer system employing the ANSIX3T11-standardized fiber channel as the interface between host computers and a storage control device and also including the host computers, the storage control device and more than one storage device under control of the storage control device, it is possible to deter unauthorized access from any one of the host computers, which in turn makes it possible to attain the intended data secrecy protection within the storage device.

In addition, it becomes possible to precisely managing those access attempts from any one of the host computers in a one-to-one correspondence manner among the host computers and storage controller ports as well as storage regions; accordingly, the storage device may be efficiently utilized to meet the needs upon alteration of the usage per storage region.

These and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention, as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram showing a hardware configuration of a first practicing form of the present invention.

Fig. 2 is a diagram showing a format of a frame in the first practicing form.

Fig. 3 is a diagram showing a format of a frame header which constitutes the frame shown in Fig. 2.

Fig. 4(A) is a format diagram of a payload of FCP_CMND which is one of frames shown in Fig. 2; and, Fig. 4(B) is a format diagram of FCP_CDB constituting the payload.

Fig. 5 shows one example of a sequence performing delivery of a data frame between a host computer and a device in the first practicing form, wherein Fig. 5(A) shows a sequence upon attempting of log-in, Fig. 5(B) is a sequence diagram when execution of a read command, and Fig. 5(C) is a sequence diagram upon receipt of a write command.

Fig. 6 is a diagram showing a control table used by a storage controller in controlling a host computer or computers in the first practicing form.

Fig. 7 shows a flow chart of frame processing as executed by the storage controller upon issuance of a log-in request from an upper-level computer (host) in the first practicing form.

Fig. 8 is a diagram showing a control table used by the storage controller for management of storage regions in the first practicing form.

Fig. 9 shows a flow chart of frame processing as executed by the storage controller upon issuance of an I/O request from the host in the first practicing form.

Fig. 10 is a diagram showing a hardware configuration in the case where the storage device under control of the storage controller is an optical disk library as a second practicing form of the present invention.

Fig. 11 is a diagram showing a control table as managed by the storage controller in the second practicing form shown in Fig. 10.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An explanation will first be given of a fiber channel and a storage system structured using the channel in accordance with the present invention with reference to Figs. 1 to 5.

Fig. 1 is a diagram showing a hardware configuration of the storage system in the case where a storage device operable under control of a storage controller unit are a disk array module or "subsystem." In Fig. 1, reference numerals 10, 20, 30 designate host computers each of which may be a central processing unit for executing data processing required.

Numeral 40 designates a storage controller unit of the disk array subsystem in which the principles of the present invention are implemented. As shown in Fig. 1, the storage controller 40 is constituted from a fiber channel control unit 41 which may be a protocol processor including a direct memory access (DMA) for controlling data transmission between it and the host computers 10, 20, 30, a microprocessor 42 for controlling all possible operations of the storage controller, a control memory 43 for storing therein microprograms for control of the operation of the controller along with control data associated therewith, a cache control unit 44 for controlling writing and reading data to and from the cache, a disk cache 45 for temporarily buffering write data and read data to/from a disk drive(s), a device interface control unit 46 which may be a protocol processor including DMA for controlling data transfer between it and its associative disk drives, and a panel 47 for use in inputting device configuration information to the storage controller.

Numeral 50 is the disk array subsystem operable under control of the storage controller 40. The disk array subsystem 50 is a device that stores therein data of host computers, which may be arranged to includes therein a plurality of individual separate disks as disposed to have certain redundancy.

The disks constituting the disk array subsystem 50 are logically divided into portions or "partitions" which may be set at specified RAID levels different from one another. The partitions are called the RAID group. This RAID group is further logically subdivided into regions that may be SCSI access units called the logical units (LUs), each of which has its unique logical unit number (LUN) adhered thereto. In this embodiment, the disk array subsystem 50 illustrated herein comes with two LUs: an LU0 (51) that is the LU indicating the number LUN0, and LU1 (52) with the number LUN1.

It is noted that the number of LUs should not be exclusively limited to the two (2) as shown in Fig. 1 and may be increased more; in the case of single target functions, the LU may be maximally increased up to eight (8) per target.

It is also noted that while in this embodiment the storage regions called the LUs are used as the access units, such storage regions each acting as the access unit may alternatively be those storage regions with a physical volume being as the unit or with a RAID group as unit.

The host computers 10, 20, 30 and storage controller 40 employ a fiber channel 60 as the interface, and are connected together via a device known as the "fabric."

An operation of the system shown in Fig. 1 will be explained under the assumption that the operation is performed in one exemplary case where the host computer 10 performs data transfer toward the disk array subsystem 50 by way of the storage controller 40. The following description will mainly deal with the flow of control and the data flow.

When the host computer 10 generates and issues an access request, the fiber channel control unit 41 recognizes such request then issuing a task interruption request to the microprocessor 42. In turn, the microprocessor 42 causes the control memory 43 to store therein both command information from the host computer and necessary control information required in this invention.

If the command information is a write command, then the microprocessor 42 instructs the fiber channel control unit 41 to execute data transfer and then stores the transferred data in the cache 45 via the cache controller 44. With respect to the host computer 10, the fiber channel control unit 41 issues a write completion report thereto. After completion of such write completion reporting, the microprocessor 42 controls the device interface controller 46 thus permitting data and redundancy data to be written into the disk array subsystem 50. In this case, during ordinary or standard RAID5 operations, a new parity is created based on the old data and old parity as well as new data; on the contrary, according to the control scheme of this invention, the microprocessor 42 does the same using the device interface controller 46 and the cache control unit 44 as well as the control memory 43 plus the cache 45.

On the other hand, upon receipt of read command information as the command information from the host computer 10, the microprocessor 42 sends an instruction to the device interface control unit 46 for providing access to the disk array subsystem 50 which stores therein the data block of this access request to read data therefrom, which data will then be stored into the cache 45 through the cache control unit 44. The microprocessor 42 issues an instruction to the fiber channel control unit 41; the fiber channel control unit 41 in turn transfers the data stored in the cache 45 toward the host computer 10 and then sends a read completion report to the host computer after completion of the data transfer required.

Next, a technical advantage of the fiber channel 60 will be explained as follows. The fiber channel may be a high-speed interface capable of transferring data at 100 MB/s at a distance of 10km in maximum. The fiber channel's architecture is designed to send data from a "source" buffer to its "destination" buffer while moving the buffer contents from one device to another in a way independent of the format and contents of data per se; accordingly, any overhead which processes different network communications protocols will no longer take place thus enabling achievement of high-speed data transmission. A variety of kinds of layers may be built in the upper-level logical layer, such as for example TCP/IP, SCSI, ESCON, IPI and the like. In other words, it does have the logical compatibility with other interfaces. The device called the fabric is expected to execute the complicated device-to-device connection/exchange function, which leads to the capability of organization of a multi-layered logical bus configuration.

The basic unit based on which the fiber channel exchanges or distributes data is called the "frame." Next, this frame will be explained with reference to Fig. 2.

As shown in Fig. 2, a frame 70 is configured from a start-of-frame (SOF) section 71, frame header 72, data field 73, cyclic redundancy check (CRC) 74, and end-of-frame (EOF) 75.

The SOF 71 is an identifier of 4 bytes which is put at the top of the frame.

The EOF 75 is a 4-byte identifier at the last location of the frame; a combination of SOF 71 and EOF 75 indicates the boundary of frame. In the fiber channel, an "idle" signal or signals flow therein in cases where any frames are absent.

The frame header 72 contains therein a frame type, host protocol type, source and destination's N_Port_ID information, N_Port_Name information and the like. The N_Port_ID is information indicative of an address, whereas N_Port_Name represents a port identifier.

The header of upper-level layer may be put at the top part of the data field 73. This is followed by a payload section which carries data per se. CRC 74 is a 4 byte check code for use in checking or verifying the frame header and data in the data field.

The frame header 72 has a format 80 as shown in Fig. 3. In the frame header format 80, a destination identifier (D_ID) 81 is an address identifier on the frame reception side, whist a source identifier (S_ID) 82 is an identifier indicative of the N_Port address on the frame transfer side, each of which may involve N_Port_ID, N_Port_Name information, etc.

An explanation will next be given of a payload 90 of fiber channel protocol command FCP_CMND, which stands for fiber channel protocol for SCSI command and which is one of payloads of the data field 73 constituting the frame, in conjunction with Figs. 4(A) and 4(B).

A logical unit number LUN for issuance of a command is assigned to an FCP logical unit number (FCP_LUN) field 91. A command control parameter is assigned to an FCP control (FCP_CNTL) field 92. And, an SCSI command descriptor block is stored in an FCP command descriptor block (FCP_CDB) field 93 for indication of a command type such as a read command "Read" or the like, an address such as LUN, and a block number. The amount of data to be transferred in response to the command is designated by byte number in an FCP data length (FCP_DL) field 94.

Data exchange/distribution operations are executed by use of the frame thus arranged as described above.

Frames employed herein may be generally classified based on function into a data frame and link control frame. The data frame is for use in transferring information, and thus has data and command as used by the host protocol, which are built in the payload section of the data field thereof.

On the other hand, the link control frame is typically used for indication of a success or failure of frame distribution. There may be a frame or the like for use in indicating actual receipt of a single frame or in notifying a parameter concerning transmission in log-in events.

Next, the "sequence" will be explained with reference to Fig. 5. The sequence in the fiber channel may refer to a collection of data frames concerned which will be unidirectionally transferred from one N_Port to another N_Port, the sequence corresponding to the phase in SCSI. A collection of such sequences is called the "exchange." One example is that a collection or group of certain sequences will be called the exchange, which sequences undergo exchange/distribution processing for execution of a command within a time period spanning from the issuance of such command to the completion of command execution (including command issuance, data transmission, and completion reporting). As apparent from the foregoing description, the "exchange" may be equivalent to I/O of SCSI.

Figs. 5(A), 5(B) and 5(C) show a log-in sequence (100), read command sequence (110), and write command sequence (120), respectively.

In the fiber channel interface, the intended communication becomes available in a particular event in which the host computer sends the device a port log-in (N_Port Login) frame containing a communication parameter, and then the device actually receives this frame. This will be called the "log-in." Fig. 5(A) shows such log-in sequence (100).

In the log-in sequence (100) shown in Fig. 5(A), the host computer first sends a PLOGI frame to the device at a sequence 101 thereby to require a log-in attempt. The device in turn sends an acknowledge (ACK) frame to the host computer thereby informing it of actual receipt of the PLOGI frame.

Then, at a sequence 102, the device operates to send the host computer either an accept (ACC) frame if the log-in request is accepted or a link service reject (LS-RJT) frame if the request is to be rejected.

Next, the read command sequence (110) of Fig. 5(B) will be explained.

In a sequence 111, the host computer sends the FCP_CMND frame to the device for requiring execution of a read operation. The device then sends back the ACK frame to the host computer.

At sequence 102, the device sends the host computer an FCP transfer ready (FCP_XFER_RDY) frame thereby notifying it of completion of preparation for data transmission. The host computer then sends the ACK frame to the device.

The routine goes next to sequence 113 which permits the device to send the host computer an FC data (FC_DATA) frame and then transfer data thereto. The host computer sends back ACK frame to the device.

At the next sequence 114, the device sends the FCP_RSP frame to the host computer to thereby inform it of successful completion of data transmission required. The host computer then sends back ACK frame to the device.

An explanation will next be given of the write command sequence (120) of Fig. 5(C).

At sequence 121, the host computer sends the device an FCP_CMND frame to perform issuance of a write request. In turn, the device sends ACK frame to the host computer.

Then at sequence 122, the device sends FCP_XFER_RDY frame to the host computer in order to inform it of the fact that data writing is available. The host computer sends ACK frame to the device.

Further, in sequence 123, the host computer sends FCP_DATA frame to the device for execution of data transfer. The device then sends ACK frame to the host computer.

Lastly at sequence 123, the device sends the host computer an FCP response (FCP_RSP) frame thereby notifying it of successful completion of data reception concerned. The host computer then sends ACK frame to the device.

While the general system configuration and format plus sequences have been explained in conjunction with Figs. 1 to 5(C), a security check scheme incorporating the principles of the present invention will be explained below.

A security check scheme will first be explained which employs the N_Port_Name information during PLOGI processing.

In accordance with the invention, a first operation to be done in Fig. 1 is that the user sets or establishes a list of one or several host computers that may provide access to the microprocessor 42 of the storage controller 40 prior to start-up of the host computers 10, 20, 30. More specifically, the N_Port_Name and N_Port_ID information capable of identifying such host computer(s) may be input using the panel 47. When this is done, in order to attain the secrecy protection function upon inputting to the panel, entry of a password should be required upon inputting of the information to thereby enhance the security.

After input of the password, if such input password matches a preset password, then input the N_Port_Name information of more than one accessible host computer with respect to each port of the storage controller to thereby store the input information in the control table.

Now, assume for example that the host computers 10, 20 are capable of getting access to the disk array subsystem 50 whereas the host computer 30 is incapable of accessing disk array subsystem 50. Assume also that the N_Port_Name is such that the host computer 10 is HOSTA, host computer 20 is HOSTB, and host computer 30 is HOSTC. Suppose that the port of the fiber channel control unit 41 of the storage controller 40 is CTL0P0. If this is the case, the resulting log-in request control table 130 is as shown in Fig. 6.

By establishing this log-in request control table 130 shown in Fig. 6 in a nonvolatile memory, it becomes possible to protect the management information against any possible power interruption or failure.

In addition, the information stored in the log-in request control table 130 is saved in the hard disk region 50 upon occurrence of power off. Or alternatively, upon updating of information, reflection is performed to the memory 43 and the disk 50. This may enable the storage controller 40 to permanently hold or store therein the information until it is subject to resetting or re-establishment.

It should be noted that while the "self" node information for use in identifying nodes and/or ports in the fiber channel may also involve N_Port_ID other than the N_Port_Name, it is desirable that the N_Port_Name information be used as an object to be checked for security. This is because of the fact that the N_Port_ID will possibly be altered or modified and is not the numeral value under management by the users.

Next, an explanation will be given of a frame processing procedure of the storage controller in reply to issuance of a log-in request from a host computer with reference to Figs. 1 and 7.

(Step S71)

The host computers 10, 20, 30 start up each issuing a PLOGI frame, which is the log-in request frame storing therein the N_Port_Name information. Upon receipt of such frame, the microprocessor 42 of the storage controller 40 sends back each host computer an ACK frame representative of actual receipt of the frame.

(Step S72)

And, the microprocessor 42 attempts to extract N_Port_Name information as stored in the frame, and then performs comparison for determining whether such N_Port_Name information has already been registered in the N_Port_Name list within the presently available preset control table.

(Step S73), (Step S74), (Step S75)

The N_Port_Name information that is presently stored in the frames issued from the host computers 10, 20 may match the N_Port_Name information which has been registered within the control table so that the microprocessor 42 of the storage controller 40 returns the ACC frame to the host computers 10, 20 as a mark of actual receipt of the individual log-in request while simultaneously continuing to execute the log-in processing.

(Step S73), (Step S76)

On the other hand, the N_Port_Name information stored in the frame as issued from the remaining host computer 30 fails to match the N_Port_Name information registered in the control table so that the microprocessor 42 of storage controller 40 returns to the host computer 30 an LS_RJT frame which contains therein a reject parameter for rejection of its connection attempt.

In the way as described above, by causing the storage controller 40 to manage the one-to-one correspondence of those ports of the host computers and the storage controller using the log-in request control table 130, it is possible for users to prevent any unauthorized access attempts from host computers on a port-by-port basis thereby maintaining enhanced security.

Next, one preferred methodology will be described which is for practicing the security check scheme using the N_Port_Name information per LUN that is the storage region of the disk array subsystem in accordance with the principles of the present invention.

In accordance with the invention, first establish a list of those accessible host computers per LUN to the microprocessor 42 of storage controller 40 before startup of the host computers 10, 20, 30. Then, input using the panel 47 certain information such as the N_Port_Name or N_Port_ID information or the like capable of identifying the host computers. When this is done, request entry of a password upon inputting of such information in order to achieve the secrecy protection function through input to the panel 47, thereby enhancing the security.

After inputting such password, if this matches the preset password, then input the port of storage controller along with the N_Port_Name information of one or several accessible host computers, thereby storing the input information in the control table.

Assume here that the LU0 (51) is accessible from the host computer 10 via a port of the fiber channel control unit 41 of the storage controller 40 whereas the LU1 (52) is accessible from the host computer 20 via a port of fiber channel control unit 41 of storage controller 40. Suppose that regarding the N_Port_Name, the host computer 10 is HOSTA while host computer 20 is HOSTB. Imagine that a port of fiber channel control unit 41 of storage controller 40 is CTL0P0. If this is the case, an I/O request control table 140 is as shown in Fig. 8.

This I/O request control table 140 shown in Fig. 8 is established in the storage space of a nonvolatile memory thereby making it possible to protect the management information against loss or destruction due to any accidental power interruption or failure.

In addition, upon occurrence of power off, the information stored in the I/O request control table 140 shown in Fig. 8 is to be stored in the hard disk region 50. Or alternatively, reflection is carried out to the memory 43 and disk 50 upon updating of information. This makes it possible to permanently hold or maintain the information until it is reestablished at later stages.

Although in this embodiment the channel path route is single, the same goes with other systems having a plurality of channel path routes.

A frame processing procedure of the storage controller in response to issuance of the I/O request from more than one host computer will now be explained in conjunction with Figs. 1 and 9. While in the prior example stated supra the security check was done in the course of PLOI, the check is performed per SCSI command in this embodiment.

(Step S91)

Where the host computer 10 desires to issue the I/O request to LU0 (51), the host computer 10 generates and issues a specific frame storing therein SCSI CDB toward the storage controller 40. Upon receiving of this frame, the storage controller 40 first sends back the ACK frame representative of actual receipt of this frame.

(Step S92)

And, the microprocessor 42 extracts the N_Port_Name information stored in the frame along with the LUN number within the CDB, and then performs comparison to determine whether such N_Port_Name information and LUN number are registered to the list within the control table which has been preset and maintained presently.

(Step S93), (Step S94), (Step S95)

Since the content "the host computer 10 can access LU0(51)" has been registered in the management table, the microprocessor 42 of the storage controller 40 receives the command and continues execution of I/O processing.

(Step S91)

On the other hand, where the host computer 20 issues an I/O request frame of LU0 (51), when the storage controller 40 does receive this frame storing therein the SCSI CDB, the microprocessor 42 first returns to the host computer 20 the ACK frame indicative of actual receipt of this frame.

(Step S92)

And, the microprocessor 42 operates to extract both the N_Port_Name information stored in the frame and the LUN number within CDB, and then executes search processing to thereby determine whether such N_Port_Name information and LUN number are present in the management table.

(Step S93), (Step S96)

Suppose that the search reveals the absence of any combination of its corresponding LUN and N_Port_Name in the management table. If this is the case, the microprocessor 42 of storage controller 40 sends an LS_RJT frame to the host computer 20 for rejection of the I/O request thereof.

In this way, the storage controller may prevent any unauthorized access attempts.

Although the explanation herein was devoted to the log-in and I/O request frames, any other information may be employed for comparison, including but not limited to the N_Port_Name information as stored in any one of the other host computer frames.

It must be noted that the storage device under control of the fiber channel connection storage controller should not exclusively be limited to the disk array subsystem stated supra, and the principles of the present invention may alternatively be applicable to any systems employing an optical disk drive, magneto-optical disk drive and magnetic tape storage as well as library apparatus including one or several of them in combination.

A summary of the case where the present invention is applied to a system including its storage device under control of the storage controller which is configured from an optical disk device or "subsystem" will be explained with reference to Fig. 10. Reference numeral 150 designates such optical disk library subsystem under control of the storage controller 40; numeral 151 indicates an optical disk drive; 152 to 156, optical disk media.

The user is expected before startup of the host computers 10, 20, 30 to make use of the panel to establish a correspondence relation among the individual medium and drive as well as port relative to the N_Port_Name information while maintaining in a microprogram the right or authorization of accessibility of host computers.

Assume that those media 152, 153, 154 are accessible from the host computer 10 whereas media D155, E156 are accessible from host computer 20. Suppose that the N_Port_Name information of host computer 10 is HOSTA, that of host computer 20 is HOSTB. Suppose also that the port of storage controller 40 is CTL0P0, that of optical disk drive A151 is DRIVE0, and those of respective media A152, B153, C154, D155 and E156 are MEDA, MEDB, MEDC, MEDD and MEDE. In this case, a request control table 160 is as shown in Fig. 11.

When respective host computers generate and issue I/O request frames, volume information must be stored in CDB in the payload constituting each frame; accordingly, the storage controller 40 is responsive to receipt of the frame for comparing both the N_Port_Name information within the frame and a medium identifier within the payload to corresponding items as presently stored in the control table which has been preset and held in the storage controller 40. In this way, applying the principles of the invention may enable the storage controller to eliminate any possible unauthorized access attempts from the host computers.

Claims

1. In a computer system including a host computer, a storage device having a magnetic disk drive, and a fiber channel connection storage controller employing an ANSIX3TT11-standardized fiber channel as an interface between the host computer and the storage device, the magnetic disk drive being operable under control of the fiber connection storage controller, the fiber channel connection storage controller comprising;

   N_Port_Name information which is information issued from the host computer for distinctly identifying the host computer is preinstalled in the storage control device prior to start-up of the host computer; the storage control device has means for permanently storing therein the information until this information is reset; after startup of the host computer, the host computer generates and issues to the storage control device a frame storing therein N_Port_Name information; the storage control device has means for comparing, upon receipt of this information, the N_Port_Name information distinctly identifying the host computer as already set and stored therein to the N_Port_Name information presently stored in a received frame; and, a fiber channel connection storage control device has means for eliminating unauthorized access from the host computer in a way such that when the comparison results in match, processing based on an instruction of the frame is continued, and when failed to match, a link service reject (LS_RJT) frame for rejection of the received frame is returned to the host computer.

2. In a computer system including a host computer, a storage device having a magnetic disk drive, and a fiber channel connection storage controller employing an ANSIX3TT11-standardized fiber channel as an interface between the host computer and the storage device, the magnetic disk drive being operable under control of the fiber connection storage controller, the fiber channel connection storage controller comprising;

N_Port Name information which is information as issued from the host computer to distinctly identify the host computer is preinstalled in the storage control device prior to startup of the host computer; the storage control device has means for permanently storing therein the information until this information will be reset; after startup of the host computer, the host computer generates and issues to the storage control device a frame storing therein N_Port_Name information; the storage control device has means for comparing, upon receipt of this information, the N_Port_Name information distinctly identifying the host computer as already set and stored therein to the N_Port_Name information presently stored in a received frame; a fiber channel connection storage control device has means for eliminating unauthorized access from the host computer in a way such that when the comparison results in match, processing based on an instruction of the frame is continued, and when failed to match, a link service reject (LS_RJT) frame for rejection of the received frame is returned to the host computer; and, the fiber channel connection storage control device also has means for setting N_Port_Name information items greater in number than or equal to a physical number of host interfaces (ports) as owned by the storage control device, that is, means for setting a plurality of N_Port_Name information items per port, and means for deterring unauthorized access from the host computer even for a multi-logical path configuration upon a fiber channel Fabric connection.

3. In a computer system including a host computer, a storage device having a magnetic disk drive, and a fiber channel connection storage controller employing an ANSIX3TT11-standardized fiber channel as an interface between the host computer and the storage device, the magnetic disk drive being operable under control of the fiber connection storage controller, the fiber channel connection storage controller comprising;

N_Port Name information which is information as issued from the host computer to distinctly identify the host computer is preinstalled in the storage control device prior to startup of the host computer; the storage control device has means for permanently storing therein the information until this information will be reset; after startup of the host computer, the host computer generates and issues to the storage control device a frame storing therein N_Port_Name information; the storage control device has means for comparing, upon receipt of this information, the N_Port_Name information distinctly identifying the host computer as already set and stored therein to the N_Port_Name information presently stored in a received frame; a fiber channel connection storage control device has means for eliminating unauthorized access from the host computer in a way such that when the comparison results in match, processing based on an instruction of the frame is continued, and when failed to match, a link service reject (LS_RJT) frame for rejection of the received frame is returned to the host computer; and, the fiber channel connection storage control device also has means for setting N_Port_Name information items greater in number than or equal to a physical number of host interfaces (ports) as owned by the storage control device, that is, means for setting a plurality of N_Port_Name information items per port, and means for deterring unauthorized access from the host computer even for a multi-logical path configuration upon a fiber channel Fabric connection; and

further characterized in that in a system having many magnetic disk volumes as in a disk array device under control of the storage control device and also having a plurality of channel path routes, the fiber channel connection storage control device has means for performing management, in a one-to-one correspondence relationship, of storage regions including a logical unit number (LUN)-based logical disk extent, a RAID group-based logical disk extent, physical volume extent and the like, ports of the storage control device, and the N_Port_Name information of an accessible host computer, and further having means for deterring unauthorized access with respect to each storage region.

4. The fiber channel connection storage control device according to claim 2, characterized in that the storage control device has means for performing table-based management and storage of the information of the correspondence among the N_Port_Name information in a way such that where the storage device under control of the storage control device is any one of an optical disk drive, magneto-optical disk drive and magnetic tape device as well as library apparatus of them, said means deals with an accessible host computer, a port or ports of the storage control device and the storage device in a mutual correspondence manner and further executes correspondence management of media in the case of library apparatus; and also has means for deterring unauthorized access from the host computer.

5. The fiber channel connection storage control device according to claim 1, characterized in that the information to be managed by the storage control device for prevention of unauthorized access from the host computer is settable using a panel.

6. The fiber channel connection storage control device according to claim 1, characterized in that the information to be managed by the storage control device for prevention of unauthorized access from the host computer is settable using a panel, and by further comprising a protection scheme for use when setting of the information.

7. The fiber channel connection storage control device according to claim 1, characterized in that the information to be managed by the storage control device for prevention of unauthorized access from the host computer is settable using a utility program of the host computer.

8. The fiber channel connection storage control device according to claim 1, characterized in that the information to be managed by the storage control device for prevention of unauthorized access from the host computer is settable using a utility program of the host computer, and by further comprising an input protection scheme for use upon setup of the information.

9. In a computer system with a channel of the network architecture type for use as an interface between a plurality of host computers and a storage control device, said system comprising more than one host computer and a storage control device as well as more than one storage device under control of the storage control device, characterized in that

host computer identification information capable of distinctly identifying the host computer is prestored in the storage control device prior to startup of the plurality of host computers, and that a channel connection storage control device is operable, upon startup of the host computer to generate and issue a frame storing therein host computer identification information and upon receiving of the frame, to perform comparison in determining whether the host computer identification information stored in the frame is already established in said storage control device to permit, when the comparison results in match, execution of processing based on the frame to continue and to reject any request when the comparison results in failure of match.

FIG. 1

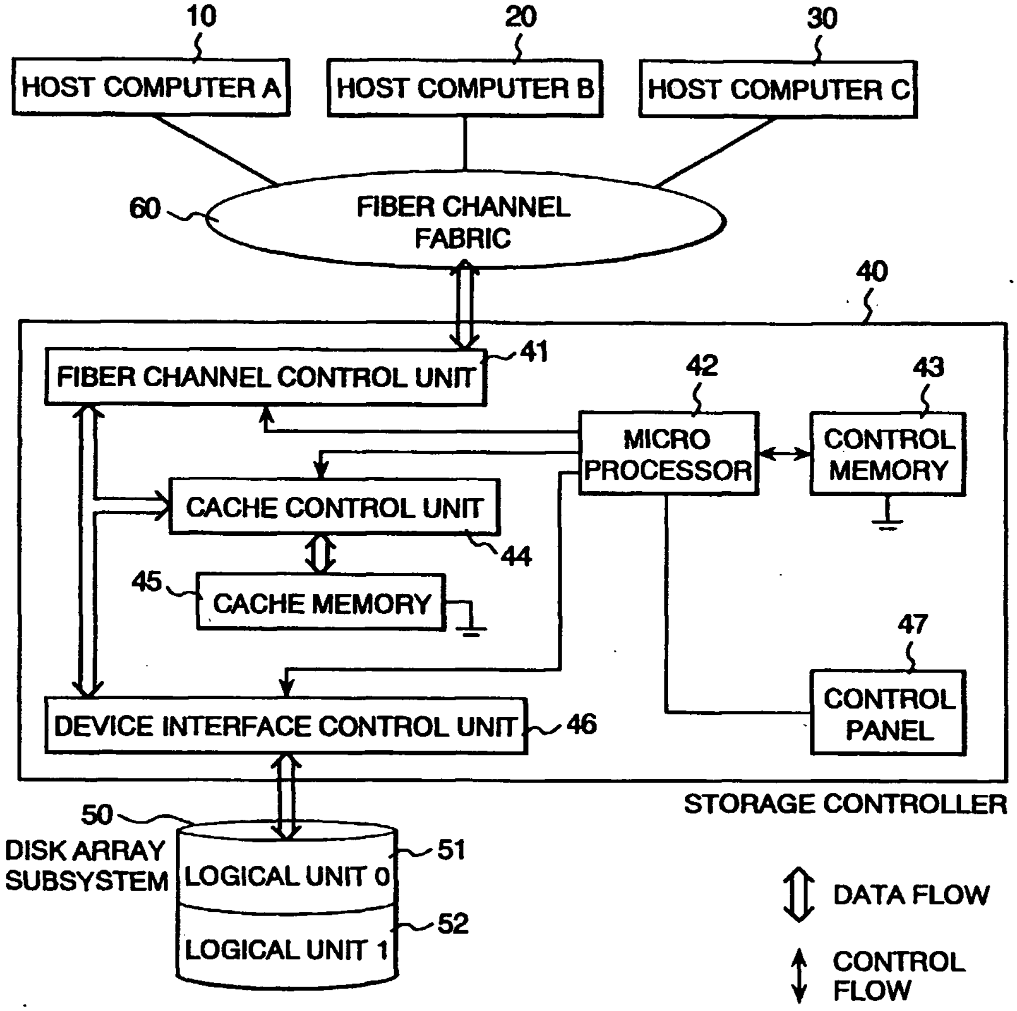

10
HOST COMPUTER A
20
HOST COMPUTER B
30
HOST COMPUTER C
60
FIBER CHANNEL FABRIC
40
FIBER CHANNEL CONTROL UNIT
41
42
MICRO PROCESSOR
43
CONTROL MEMORY
CACHE CONTROL UNIT
44
45
CACHE MEMORY
47
CONTROL PANEL
DEVICE INTERFACE CONTROL UNIT
46
STORAGE CONTROLLER
50
DISK ARRAY SUBSYSTEM
LOGICAL UNIT 0
51
LOGICAL UNIT 1
52
DATA FLOW
CONTROL FLOW

FIG. 2

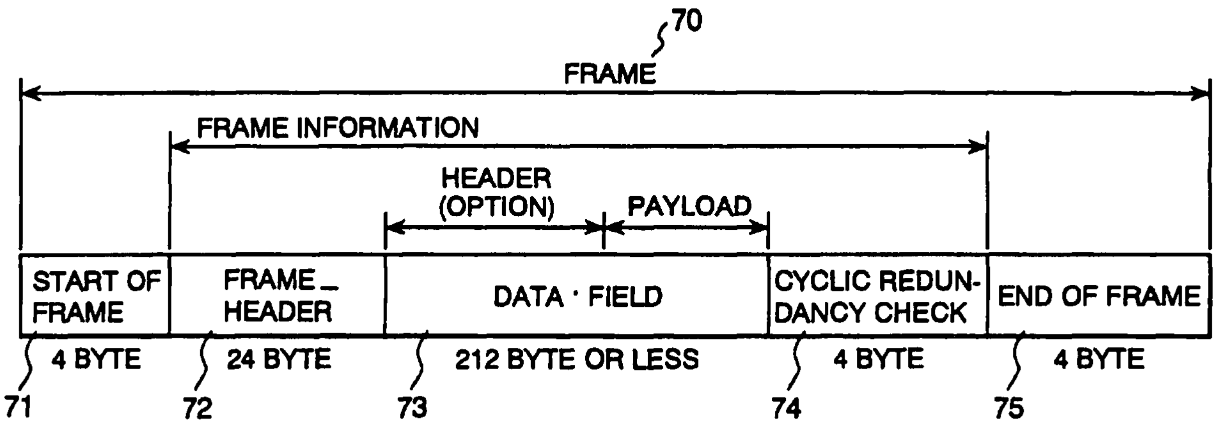
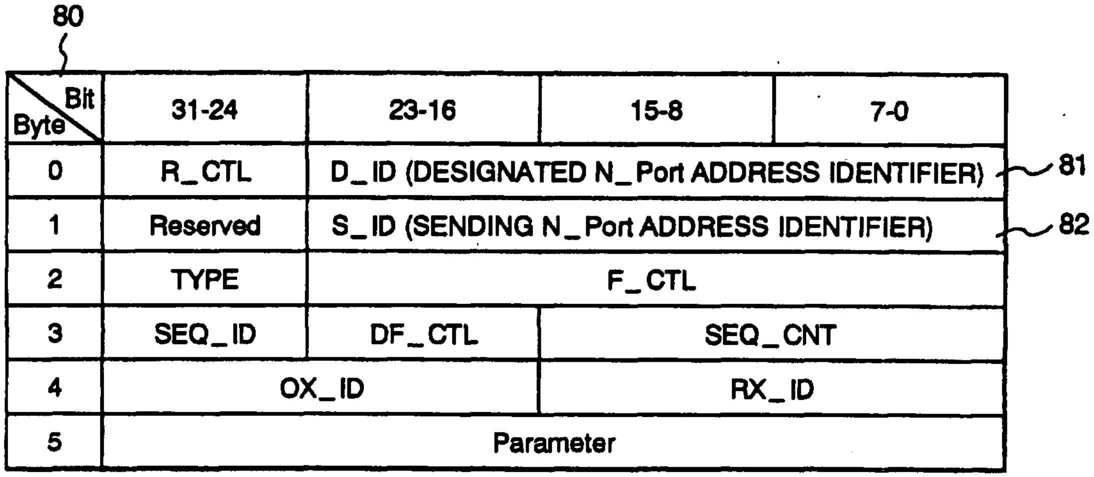

70
FRAME
FRAME INFORMATION
HEADER
(OPTION)
PAYLOAD
START OF
FRAME
FRAME_
HEADER
DATA · FIELD
CYCLIC REDUN-
DANCY CHECK
END OF FRAME
4 BYTE
24 BYTE
212 BYTE OR LESS
4 BYTE
4 BYTE
71
72
73
74
75

FIG. 3



Bit Byte	31-24	23-16	15-8	7-0
0	R_CTL	D_ID (DESIGNATED N_Port ADDRESS IDENTIFIER)		
1	Reserved	S_ID (SENDING N_Port ADDRESS IDENTIFIER)		
2	TYPE	F_CTL		
3	SEQ_ID	DF_CTL	SEQ_CNT	
4	OX_ID		RX_ID	
5	Parameter			

FIG. 4A

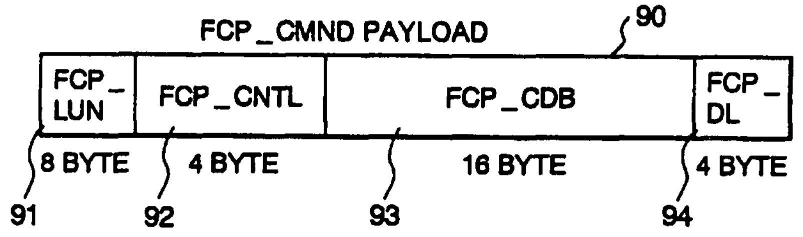


FIG. 4B

93

Byte \ Bit	7	6	5	4	3	2	1	0
0	Operation Code							
1	Logical Unit Number			Logical Block Address (MSB)				
2	Logical Block Address							
3	Logical Block Address (LSB)							
4	Transfer Length							
5	Vendor Unique		Reserved				Flag	Link

FIG. 5A

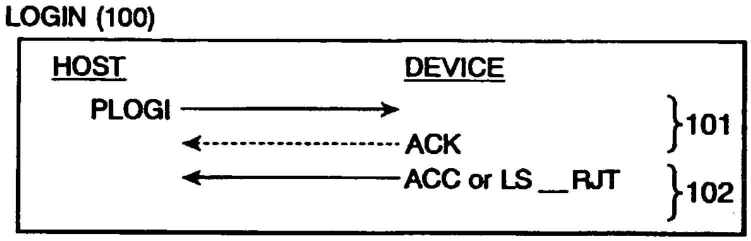


FIG. 5B

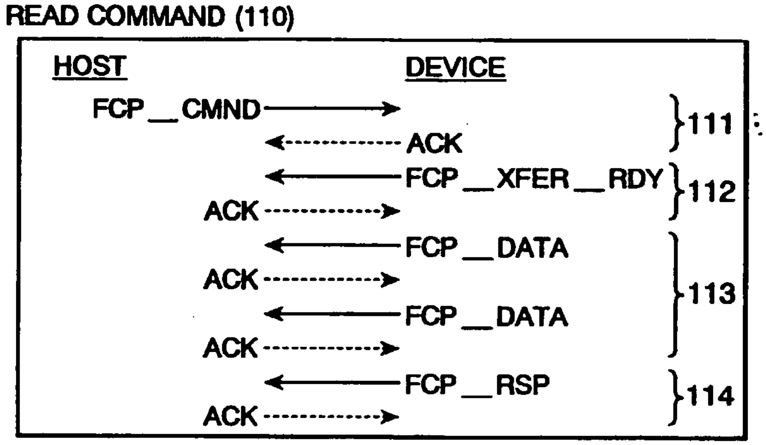


FIG. 5C

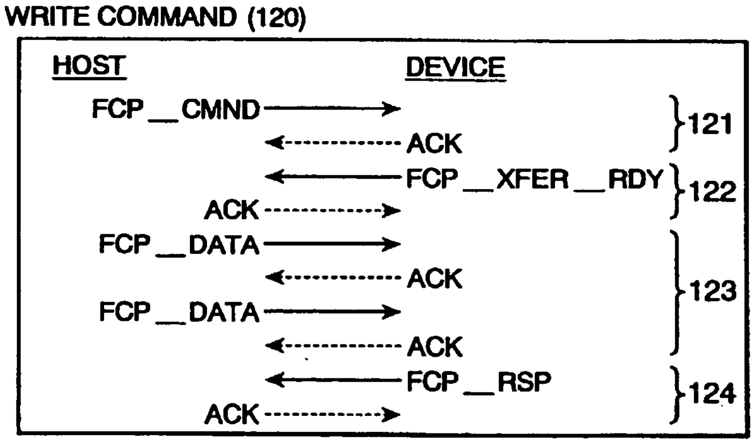


FIG. 6

CONTROL TABLE 130

HOST N__Port __Name	HOST INTERFACE (OR PORT) ON STORAGE CONTROLLER
HOSTA	CTL0P0
HOSTB	CTL0P0

FIG. 7

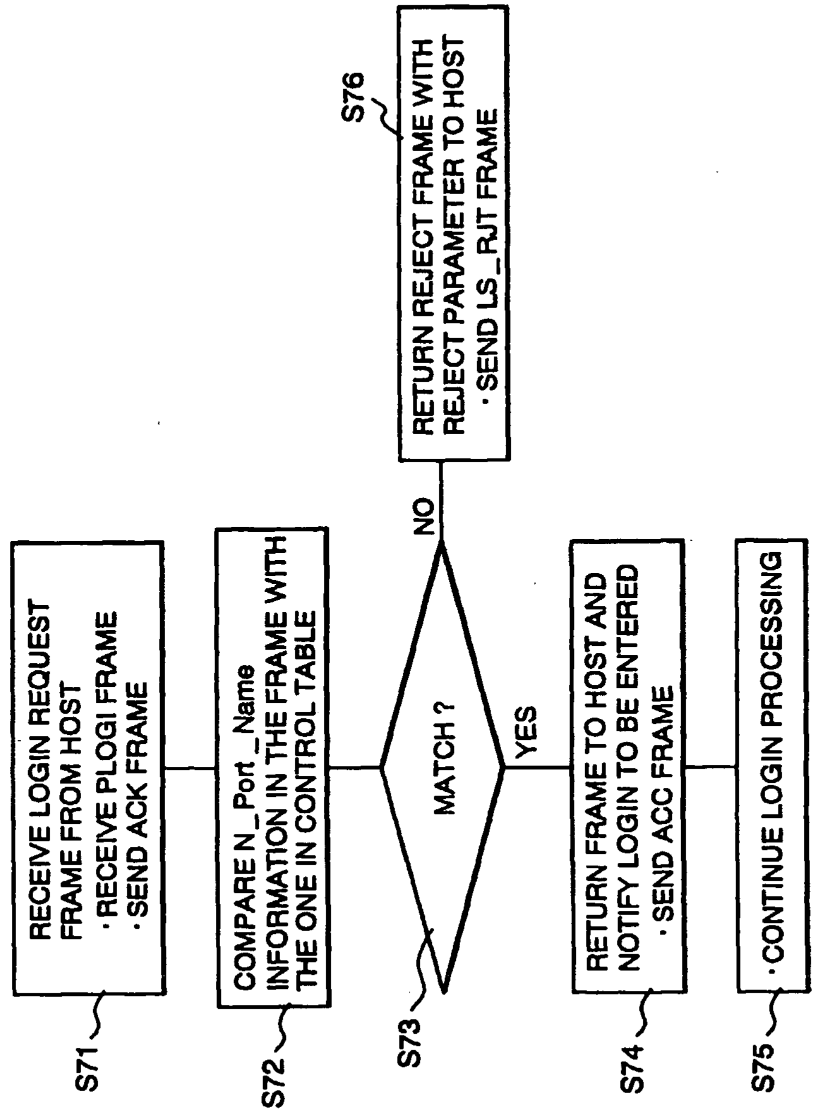

S71
RECEIVE LOGIN REQUEST FRAME FROM HOST
· RECEIVE PLOGI FRAME
· SEND ACK FRAME
S72
COMPARE N_Port_Name INFORMATION IN THE FRAME WITH THE ONE IN CONTROL TABLE
S73
MATCH ?
NO
S76
RETURN REJECT FRAME WITH REJECT PARAMETER TO HOST
· SEND LS_RJT FRAME
YES
S74
RETURN FRAME TO HOST AND NOTIFY LOGIN TO BE ENTERED
· SEND ACC FRAME
S75
· CONTINUE LOGIN PROCESSING

FIG. 8

CONTROL TABLE 140

STORAGE REGION LOGICAL UNIT	HOST N__Port __Name	HOST INTERFACE (OR PORT) ON STORAGE CONTROLLER
LOGICAL UNIT 0	HOSTA	CTL0P0
LOGICAL UNIT 1	HOSTB	CTL0P0

FIG. 9

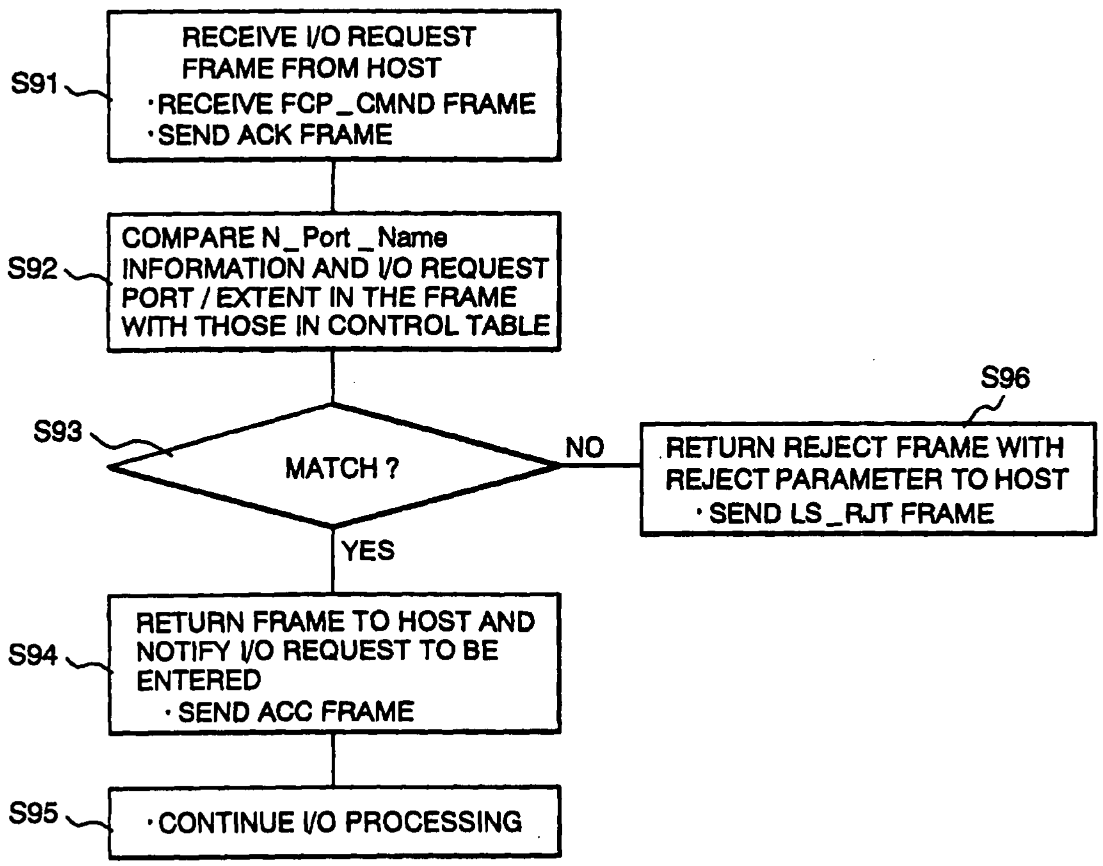

S91
RECEIVE I/O REQUEST FRAME FROM HOST
·RECEIVE FCP_CMND FRAME
·SEND ACK FRAME
S92
COMPARE N_Port_Name INFORMATION AND I/O REQUEST PORT / EXTENT IN THE FRAME WITH THOSE IN CONTROL TABLE
S93
MATCH ?
NO
YES
S96
RETURN REJECT FRAME WITH REJECT PARAMETER TO HOST
·SEND LS_RJT FRAME
S94
RETURN FRAME TO HOST AND NOTIFY I/O REQUEST TO BE ENTERED
·SEND ACC FRAME
S95
·CONTINUE I/O PROCESSING

FIG. 10

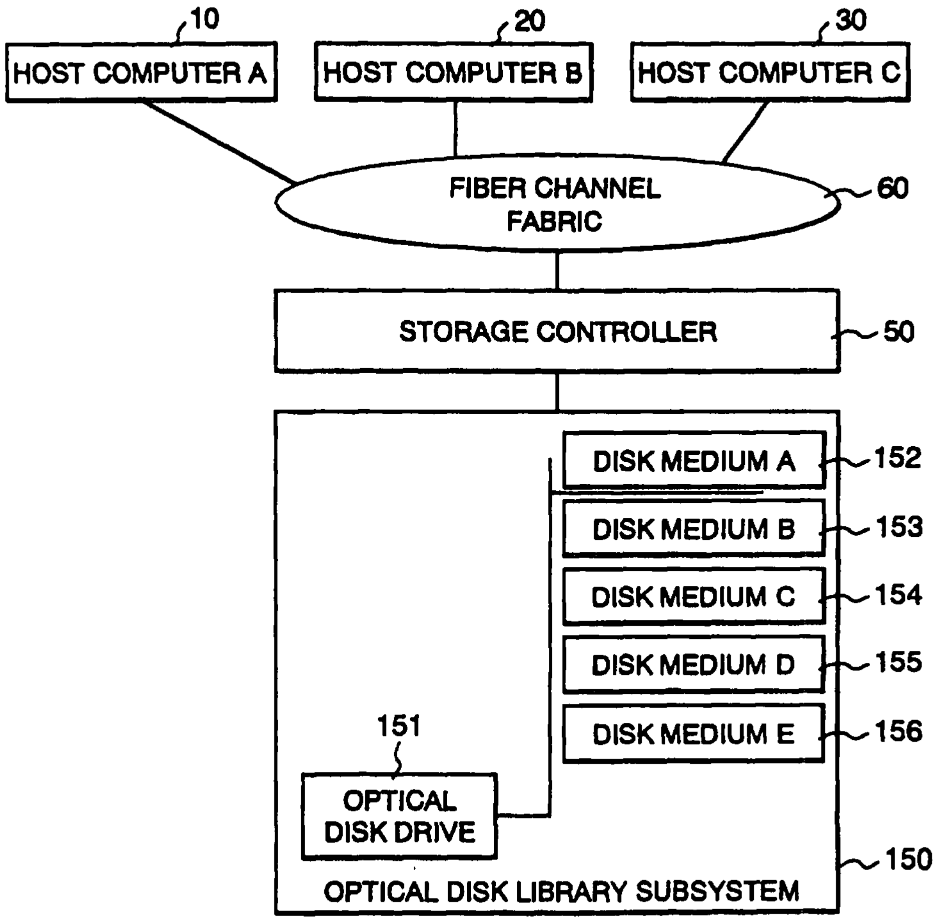

10
HOST COMPUTER A
20
HOST COMPUTER B
30
HOST COMPUTER C
FIBER CHANNEL FABRIC
60
STORAGE CONTROLLER
50
DISK MEDIUM A
152
DISK MEDIUM B
153
DISK MEDIUM C
154
DISK MEDIUM D
155
DISK MEDIUM E
156
151
OPTICAL DISK DRIVE
150
OPTICAL DISK LIBRARY SUBSYSTEM

FIG. 11

CONTROL TABLE 160

STORAGE REGION OPTICAL DISK MEDIUM	OPTICAL DISK DRIVE	HOST N__Port __Name	HOST INTERFACE (OR PORT) ON STORAGE CONTROLLER
MEDA	DRIVE0	HOSTA	CTL0P0
MEDB	DRIVE0	HOSTA	CTL0P0
MEDC	DRIVE0	HOSTA	CTL0P0
MEDD	DRIVE0	HOSTB	CTL0P0
MEDE	DRIVE0	HOSTB	CTL0P0